International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G08B

A2

(11) International Publication Number: WO 99/06974

(43) International Publication Date: 11 February 1999 (11.02.99)

(21) International Application Number: PCT/US98/15947

(22) International Filing Date: 31 July 1998 (31.07.98)

(30) Priority Data:
60/054,354 31 July 1997 (31.07.97) US

(71) Applicant (*for all designated States except US*): SPRING TECHNOLOGIES, INC. [US/US]; Suite 220, 803 W. Broad Street, Falls Church, VA 22046 (US).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): MANN, Stewart, M. [US/US]; 124 S. Spring Street, Falls Church, VA 22046 (US). MANN, L., Maribel [HN/US]; 124 S. Spring Street, Falls Church, VA 22046 (US). DURELL, Jack [US/US]; 706 Belgrove Road, McLean, VA 22101 (US).

(74) Agent: SMITH, Evan, R.; Greenberg Traurig, 8180 Greensboro Drive, McLean, VA 22046 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEM AND METHOD FOR ROBBERY PREVENTION

(57) Abstract

An access control system (100) has a biometric characteristic sensor (104) that measures stable physical characteristics of a person seeking access to a controlled area. At the same time, an affective sensor (106) measures a physiological response of the individual which varies with the individual's level of shock, fear or apprehension. An access controller (112) permits access to the controlled area only if the individual is biometrically identified as an authorized person, while at the same time the person's physiological response as measured by the affective sensor indicates that the person is not experiencing an undue level of shock, fear, or apprehension such as would be expected if the person was being held at gunpoint or otherwise being coerced.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SYSTEM AND METHOD FOR ROBBERY PREVENTION

FIELD OF THE INVENTION

This invention relates generally to the field of security for objects and personnel, and to the prevention of robbery and other crimes. The system operates generally by detecting physiological reactions to coercion, and preventing a person under coercion from accessing a secured location or facility, such as a vault, cash drawer, or financial transaction station.

BACKGROUND OF THE INVENTION

Security of banks and other concerns which conduct transactions in currency, valuables or other negotiable instruments continues to pose an increasingly frustrating problem for all.

Banks, retailers and others who remain easy prey are left with little choice but to accept the abuse, insure heavily and save face with their customers to the greatest degree possible. Similarly, despite admirable efforts and dedication, law enforcement remains stymied in the struggle to control violent robberies. The threat of prosecution is clearly not enough of a deterrent.

The fact remains that any person so motivated to write a threatening note, purchase a squirt gun or, as in most instances, brandish a loaded firearm can ordinarily flee the scene of a robbery with substantial cash. With increasing frequency the robberies are accompanied by physical assaults and

murders. For decades banks have instructed their employees to offer no resistance, and common knowledge among criminals has established banks as among the easiest of targets.

A strong need exists to provide such concerns with a robbery-free environment in which to conduct business. Specifically there exists the heretofore unaddressed need to remove from those environments the single integral element requisite to the success of such robberies; the possibility of coercing cooperation.

Past efforts in this field have provided no practical article, method or system which accomplishes reliable and consistent results. Such problems are overcome by the improvements afforded by this invention. Certain recent efforts in this field are directed toward trapping the robber in the facility upon the perceived notion that they will be unable to harm other customers or employees when contained behind reinforced materials.

Herein lies the fatal flaw. Robbers are in the business of force and understand it well. Methods will be discovered, indeed already exist to overcome such reinforcing materials. Far better than to trap an angry robber with a gun or explosives is to clearly convince them there is no chance for success before the event occurs.

One object of this invention is to prevent robberies by removing the opportunity for cooperation.

Another object is to provide a more secure environment for customers and employees.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides an anti-robbery security control which performs in response to monitored physiological changes in the human body which occur in response to fear and intimidation. The operation of the system will be described first by reference to Figure 1, which is a block schematic diagram of a preferred embodiment of the robbery deterrent system of the present invention.

Robbery deterrent system 100 includes an electronic storage site 102 wherein there are stored previously recorded biometric data corresponding to stable physical characteristics of a person. Previously recorded affective bioresponse data corresponding to the same person is also stored. The term "affective bioresponse" is used herein to describe a physiological parameter which varies according to the person's current emotions. The stored data for affective bioresponse include at least a measurement for the person when the person is not experiencing fear, shock, or a high level of stress (i.e. a "normal" measurement). Since different individuals may respond in different degrees to fear, the stored data may also include a measurement taken when the person was suddenly placed in a state of fear.

A biometric sensor 104 is provided for capturing, in real time, biometric data reflecting stable physical characteristics corresponding to a physical characteristic of a person. An affective bioresponse sensor 106 is provided for detecting physiological responses to emotions, such as fear. Affective sensor 106 may employ a variety of known sensor technologies. For example, sensor 106 may collect real time body vital sign measurements

of the person, such as pulse rate, blood pressure, blood volume pulse, respiration rate or optical response. Affective sensor 106 may also incorporate a galvanic skin response sensor, or an electromyogram sensor. If desired, affective sensor 106 may collect more than one type of measurement and correlate the different parameters for more accurate identification of a fear or stress response, in which case corresponding multiple types of data will also be stored in electronic storage 102. What is important is that affective sensor 106 is capable of detecting any of a variety of physiological characteristics of the person that will inherently change when the person is subjected to sudden fear and stress, such as during a robbery. As long as this requirement is met, any desired type of sensor may be used.

An encoder 108 is connected to biometric sensor 104 and affective sensor 106, and converts data from the form provided by the sensors to a digital data format, preferably similar to the format used to store previously recorded data in electronic storage 102. Comparator 110 is connected to encoder 108, and determines a degree of correspondence between the captured real time physical characteristic data from biometric sensor 104 and the stored physical characteristic data. Comparator 110 also determines a degree of correspondence between the captured real time body response detected by affective sensor 106 and the stored physiological responses in electronic storage 102. Comparator 110 compares the real time body response to the stored "normal" response to determine whether it is likely that the person being sensed is in an unusual state of fear. Comparator 110 may also compare the real time response to a stored "fear" response. Comparator 110 then

determines as a binary condition whether or not the person is being coerced, by threat of force, to provide access to a controlled space or transaction.

Access control circuit 112 is connected to comparator 110 and has a control output 114. Access control circuit 112 generates a signal at output 114 indicating whether access to a controlled space or transaction should be provided. Access control circuit 112 also has an input 116 which receives a signal requesting that access be provided. This signal may be used by access controller 112 to initiate operation of the sensors 104 and 106 and a comparison operation by comparator 110.

Access control circuit 112 allows access to the secured area, object, or transaction, based on a determination of whether the individual present at the station and their vital signs conform to expected values. If the individual's stable biometric characteristics do not match those of an authorized individual, or measurements of variable vital signs associated with that individual do not match expected recorded values because the individual is experiencing great fear or stress, access to the secured item, area, or transaction is prevented.

Output 114 is connected to provide a control signal to an existing control circuit for providing access to the secured space or transaction. For example, output 114 may be connected to known circuits which selectively control access. For example, appropriate known control circuits which can operate with access controller 112 may provide access to vaults, disable an alarm system, release a cash drawer latch (such as in a cash register), or enable an automatic teller machine transaction. Such control circuits are modified so that the presence of an access authorization signal on output 114 is a prerequisite to providing access.

Biometric sensor 104 captures real time data corresponding to a stable physical characteristic of a person such as a fingerprint, palm print, full facial image, features of the iris of the eye, eye retinal pattern, body thermal image, or DNA pattern. Verification of personal identification includes capturing the real time stable physical characteristic image directly from a person; encoding the image; and comparing the encoded image to stored physical characteristic data at the storage site. If the captured image is not recognized as corresponding to any of the stored data access is denied. Biometric sensor 104 may rely on any stable physical characteristic or on a combination of such characteristics for identification purposes. What is important is that the characteristic or characteristics chosen be capable of uniquely identifying an individual as an authorized individual, within an acceptable margin of error.

If the real time captured image does correspond to a predetermined degree with stored stable physical characteristic data a real time affective measurement is then captured from that person. If the captured physiological measurement fails to achieve a predetermined degree of correspondence with stored data for that person, access is denied. When the captured real time physiological response measurement does meet a predetermined degree of correspondence with stored data for that person, access to a controlled space, area, or transaction is then granted. Such a controlled space might include a cash drawer, safe, vault, secure space inside or outside, or the point of ingress or egress of a building. Such transactions might include automated teller machine functions, network access such as access to the internet, computer access, or the like.

The extremely high reliability of stable physical characteristic identification provides positive identification of an employee and allows the capture of real time physiological data from that person. These two steps are requisite to any employee prior accessing a cash drawer, vault or secured area. Preferably, there is no manual override available at the location. Thus, if a robber enters a facility such as a back and brandishes a gun, the tellers will be unable to access any cash because their physiological response to the threat will shut down access to the drawers.

The encoding, electronic storage, comparison, and access control functions of system 100 are preferably implemented in a general purpose computer such as an IBM-compatible personal computer, or may be implemented as a special purpose electronic computing circuit. Biometric sensor 104 and affective sensor 106 are connected to the computer or computing circuit through an appropriate interface card or circuit, which may incorporate encoder 108.

The method of operation of the system shown in Figure 1 will now be described in further detail with reference to the flowchart of Figure 2, which shows a preferred operating method according to the present invention. Operation of the program is initiated in Block 1, where the system receives a request to begin a transaction or provide access. As a result, control passes to Block 2, where the biometric sensor 104 (shown in Figure 1) is activated to collect an image or other data set of a stable identifying physical characteristic of the person. In block 3, the collected identifying information is compared to a database of stored identifying patterns of persons authorized to access the system. If a match is found (block 4) the person is identified and

control passes to block 5, where that person's stored vital sign or other affective physiological measurement record is retrieved. If no match is found, control passes to block 8 and access is denied.

In block 5, the affective sensor is actuated and a vital sign or other real time physiological response is measured. Then, in block 6, the physiological measurement is compared to the stored standard measurement for that person. If the stored non-fear measurement and real-time measurement do not correspond within a reasonable level of variation, i.e. if the person exhibits physiological reactions indicative of a high level of fear or stress, control passes to block 9 and access is denied. Otherwise, control passes to block 7 and access is granted.

Referring again to Figure 1, it is important that biometric sensor 104 and affective sensor 106 be arranged or controlled so that the sensors cannot be deceived by the sensing of two different persons at the same time. In other words, the sensors should be arranged or controlled with means for preventing one person from interfacing with biometric sensor 104 while a different person (such as a criminal) interfaces with affective sensor 106.

Figure 3 shows three examples of embodiments which provide means for preventing one person from interfacing with biometric sensor 104 while a different person (such as a criminal) interfaces with affective sensor 106. Figure 3A shows a circuit 302 which detects body continuity between a first sensing point and a second sensing point. A harmless low voltage, low current signal is provided to the body at one sensor point (shown as an iris scanner used as biometric sensor 104) and is detected at the other sensor location (shown as a finger sensor for galvanic skin response) to verify that

the same individual is in contact with both sensors. The verification circuit is connected to access controller 112 (shown in Figure 3) and prevents access unless the same individual is sensed by both sensors.

Figure 3B shows an integral combination sensor which visually detects a fingerprint using a fingerprint sensor as biometric sensor 104, and at the same time, measures galvanic skin response, pulse rate, or blood volume pulse using affective sensor 106. Sensor unit 304 has a housing 305 with a finger hole 306 which encloses the sensors yet permits access of a single finger to contact both sensor 104 and sensor 106. Because of the construction of this sensor, it is physically impossible to present a different finger to each sensor, and thus impossible to present more than one person's finger to the sensors at a time.

Figure 3C shows a similar arrangement wherein an iris scanner is used as biometric sensor 104 and is integrally mounted with a galvanic skin response, pulse measurement, or blood volume pulse sensor as affective sensor 106. A unified housing 308 positions the sensors in fixed relative positions. The affective sensor may be located in the temple area, for example, so that it is physically impossible to present one person's eye to the iris scanner while presenting another person's temple to the affective sensor.

In each of the embodiments of Figures 3A, 3B and 3C, the measurements of biometric sensor 104 and affective sensor 106 are taken simultaneously or almost simultaneously, so that it is impossible to substitute a different person during the sensing process depicted in Figure 2.

Fear and intimidation are the essential elements upon which assailants rely in order to achieve the short term participation and cooperation requisite

to a successful robbery. Robbers understand very well the necessity for establishing immediate authority and control over their victims by terrorizing them in the first moments of the assault.

However, all humans and particularly these victims respond in kind to acts of terror which instill such fear and intimidation. Persons confronted with such an event respond with an instant and dramatic elevation of body vital signs. Such an event and the resulting physiological response is unmistakable and any access to secured areas is denied upon such a showing.

Robbers will not go where there is demonstratably no chance for success. They do not seek a platform upon which to voice grievances or make political statements. They understand fear and force. Further attempts or increased force in this environment only serve to reinforce the operation of the system.

Thus, an improved system and method for deterring robberies and coercion has been disclosed.

We claim:

1. An access control system for selectively permitting access to a protected area by an authorized individual, comprising:

storage means for storing a database containing physical characteristic records and affective response data of individuals authorized to access the protected area;

biometric detection means connected to said storage means for detecting a physical characteristic of an individual seeking access to the protected area and positively identifying the individual by comparing the detected physical characteristic to said physical characteristic records in said database;

affective detection means for measuring a biological response of said individual seeking access to the protected area and determining whether that biological response indicates a level of emotional response indicating possible coercion; and

control means connected to said biometric detection means and said affective detection means for selectively generating an access authorization signal to control access to the protected area, said access authorization signal generated only when said biometric detection means confirms that the individual seeking access is authorized and said affective detection means indicates that the individual does not have a level of emotional response indicating possible coercion.

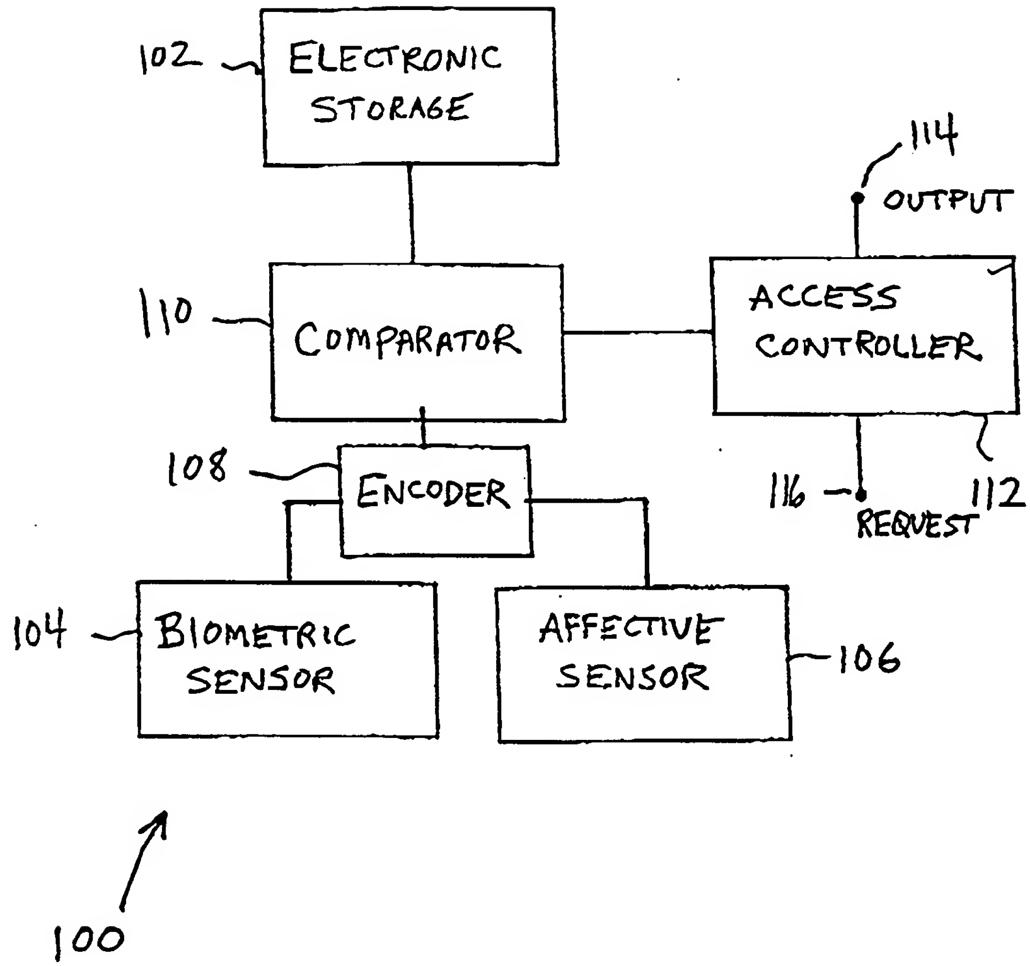
102
ELECTRONIC STORAGE
114
OUTPUT
110
COMPARATOR
ACCESS CONTROLLER
108
ENCODER
116
REQUEST
112
104
BIOMETRIC SENSOR
AFFECTIVE SENSOR
106
100

Fig. 1

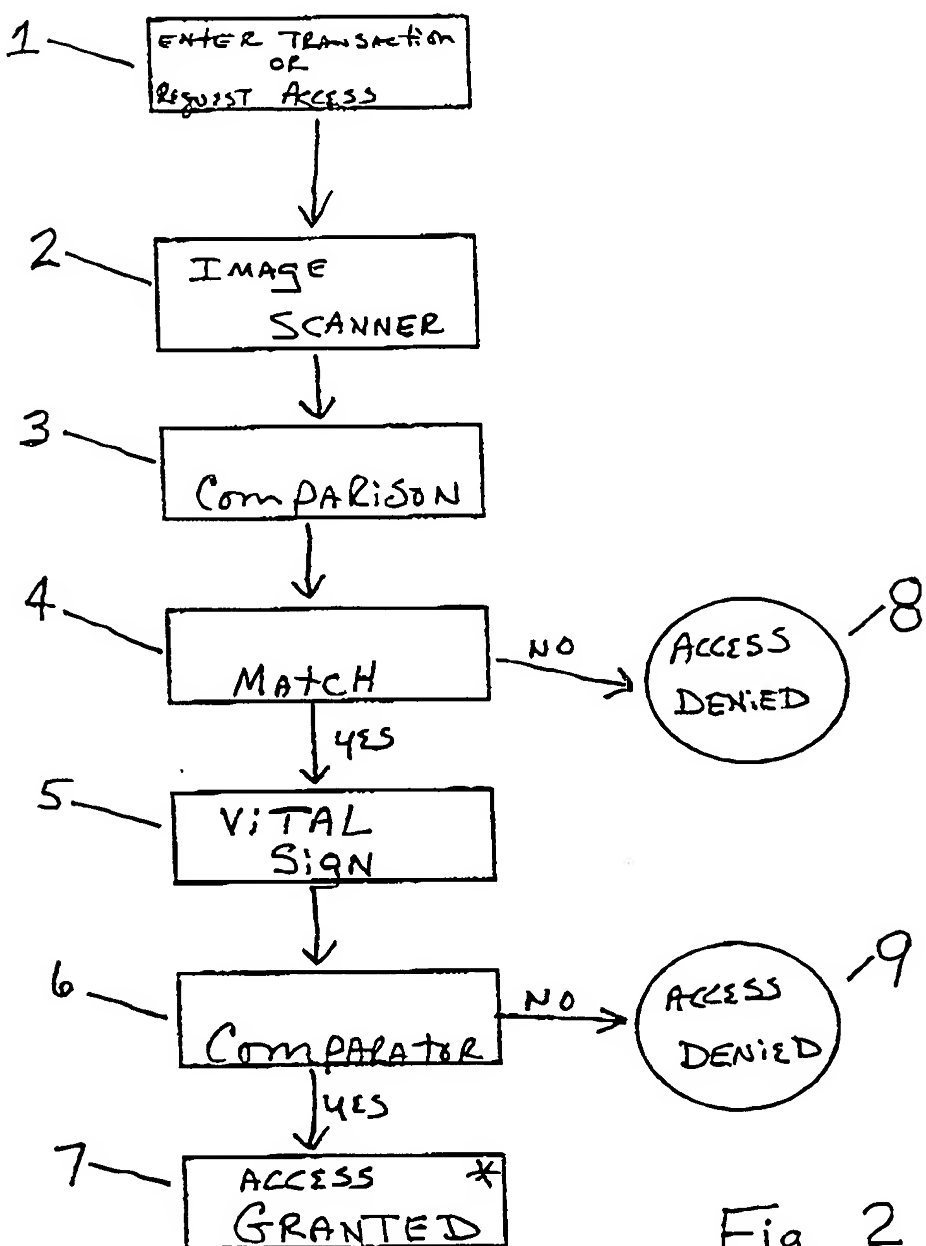
1
ENTER TRANSACTION
OR
REQUEST ACCESS
2
IMAGE
SCANNER
3
COMPARISON
4
MATCH
NO
ACCESS
DENIED
8
YES
5
VITAL
SIGN
6
COMPARATOR
NO
ACCESS
DENIED
9
YES
7
ACCESS *
GRANTED

Fig. 2

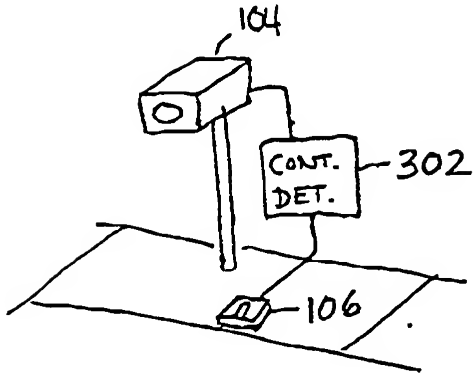

Fig. 3A

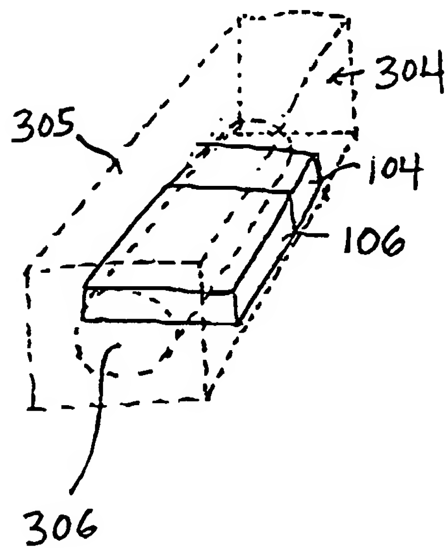

Fig. 3B

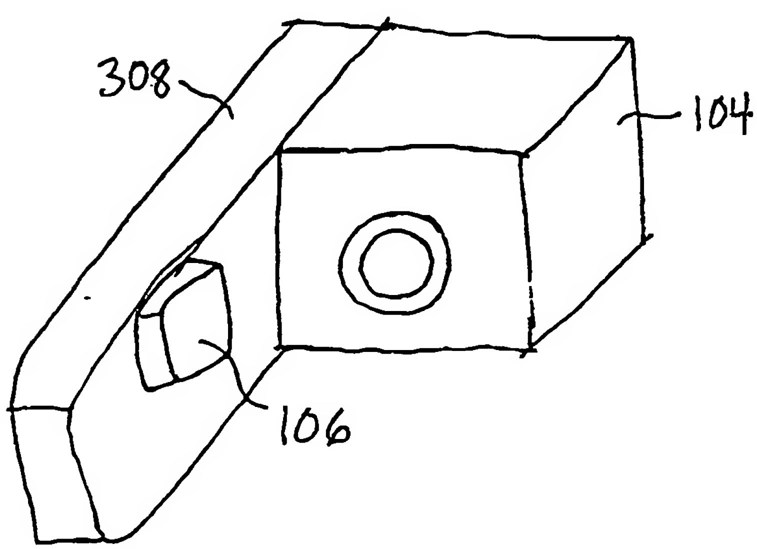

Fig. 3C